# Mobile device management

*By CPT Christopher J. Braunstein*

The modern era of computing has been shaped by the mobility revolution.

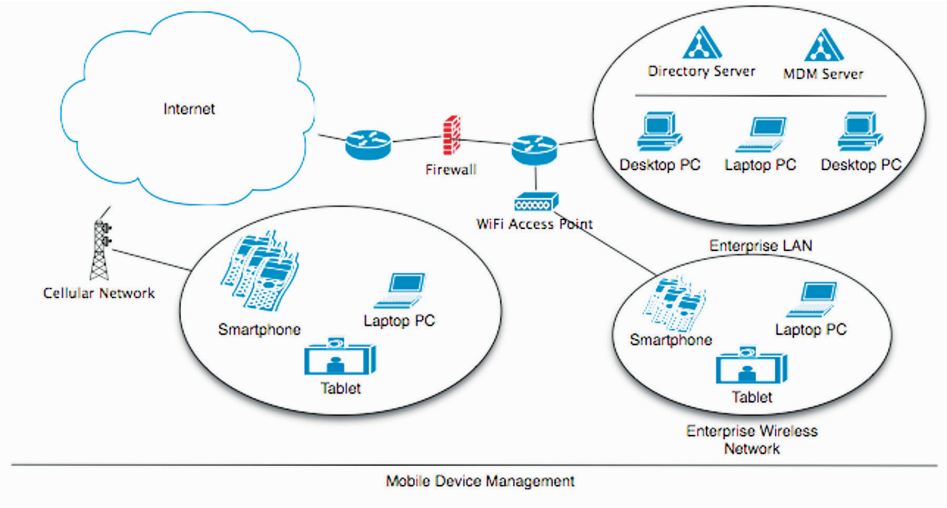
Desktops are beginning to fade in prominence as laptops, netbooks, ultrabooks, and other portable computers take over.

The pursuit of Moore's Law indicates that in the history of computing, the number of transistors that can be placed inexpensively on an integrated circuit doubles approximately every two years. This fact has resulted in an explosion of a new class of portable computers like Smartphones and tablets that are beginning to take hold in the enterprise.

Information technology departments have been flooded with radical new management ideas such as "Bring Your Own Device." Information assurance and computer security have become central concerns in every organization.

The challenges of managing a multitude of computing devices and maintaining the balance between security and usability become more complex every day.

Systems management has long been the cornerstone of enterprise-wide administration. A large organization like the Army has a clear requirement to create automated centralized processes to save time and money, increase productivity and application access, and provide a secure computing environment that minimizes risk. Management tools and processes have evolved from rudimentary programs such as shell scripts created by administrators into complex platforms and product lines. Solutions from multiple companies allow for security management, server availability monitoring, software inventory and installation, anti-virus and anti-malware management, network capacity and utilization monitoring, and user activity monitoring. Using a combination of these tools, an organization's managers can enact and enforce enterprise information technology policies and procedures.




Traditional desktop management evolved out of network management initiatives. Client desktops connected to local area networks that provided services required by users. These were often simple services like a corporate portal or file sharing. As software and operating systems evolved, the concept of a "managed desktop" became popular. Using Microsoft's Active Directory (or other open source tools such as Open Directory for Linux/Unix based computers) system administrators could apply policies to desktops. These policies could be linked to a user or to a particular policy. A managed desktop system could also provide authentication and authorization to all services included in a network.

Policies evolved over time allowing for fine-grained control over every aspect of the user's experience. Administrators could ensure a computer's software was up-to-date on patches and anti-virus definitions. They could remotely install new software on a group of desktops. Security could be enhanced by mandating password policies (or smart card authentication), disabling components of the operating system that were deemed unsafe, allowing users to only install and run approved applications, and actively monitoring the desktop's state. The policies could be applied to computer systems or to users and groups of users allowing great flexibility in the implementation of a desktop management corporate policy.

Over time, desktop computers faded and laptops became the hallmark of corporate use. Lightweight and portable laptops allowed traveling users to con-

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2012** | | **00-00-2012 to 00-00-2012** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Mobile device management** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**U.S. Army Signal Center of Excellence and Fort Gordon,Army Communicator,Signal Towers (Building 29808), Room 713,Fort Gordon,GA,30905-5301** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **3** | |

tinue to get work done on the road. Administrators provided Virtual Private Network support to allow laptop users to connect to the corporate LAN and access services that were not publicly available on the internet. Desktop policy would be enforced and updated when the user connected their laptop to the VPN. Some risk was assumed as laptops were now able to be connected to external networks, losing the protection and monitoring ability of the corporate LAN when not connected to a VPN. System Administrators had to become more vigilant in enforcing IT policies and ensuring laptop computers were up to date.

Continuing along this theme, smartphones and tablets have arrived which bring ever smaller form factors that are highly portable to the fold. Cellular networks keep these devices attached to the internet continuously allowing for data consumption at any time, but also greatly expanding the risks of attack by malicious software and users. Mobile operating systems are often limited in their management capabilities (although this is improving quickly).

Traditional desktop management systems either do not support mobile devices or have a completely different way of management, as most mobile devices use operating systems that use different security models and systems than desktops. Mobile devices are difficult to track as they move on and off of a corporate LAN or change physical locations quickly. There are many different models, operating systems, and cellular network carriers adding to the complexity.

A new tool, Mobile Device Management, has evolved that can mitigate a lot of these risks. Mobile Device Management optimizes the functionality and security of a mobile device in relation to corporate policy; much like desktop management does in traditional IT settings. Typical MDM solutions include a server component that can send messages and commands to a mobile device, and a client component which runs on the handset or tablet and implements the commands. Newer solutions do not require a client component, as the client is embedded into the mobile operating system by the software or device manufacturer. The server solution can be hosted as a corporate service on existing infrastructure, or hosted through cloud services provided by the vendor.

In order to enable a device for management it must be provisioned. This process can vary from different vendor solutions, but it is commonly accomplished by visiting a web page or installing an application from a public market. Once this client application or configuration profile is installed the device is linked to the MDM console (which is often Web-based for ease of use). The MDM administrator can then push a profile to the device over the air that would alter the configuration of the device. The contents of the profile can include device settings, network and VPN configurations, account settings, security policies, password/passcode requirements, reporting requirements, and more. These profiles can also be sent to a group of devices or group of users, depending on what the administrator is trying to accomplish. MDM solutions often collect a lot of data from the mobile device.

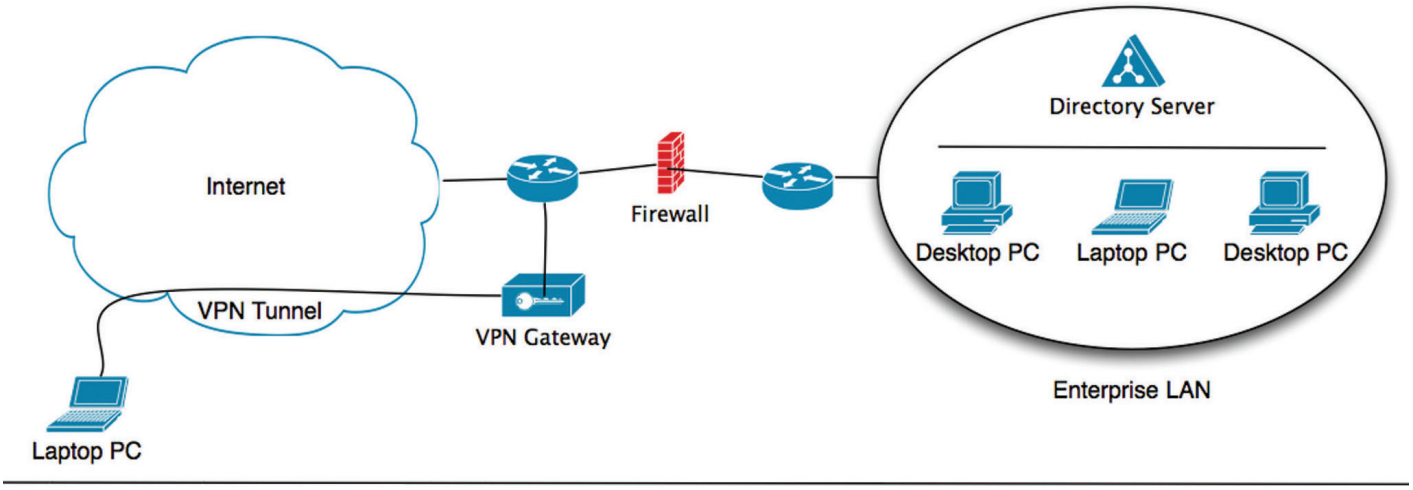
Global Positioning System embedded in the device is used for geo-location data. A summary of all settings and device conditions can be retrieved. A listing of messages/calls sent and received and their durations, software apps installed, and security state of the device can also be pushed to the MDM console. All of these things combined with the ability to control almost every aspect of the device's configuration leads to some interesting and novel thought about how to manage a network of computing devices.

An administrator can develop a system of profiles that increase or decrease permissions and security levels based not only on the user's authorization but also based on the state and location of the device or even the network to which it is connected. Tying these requirements to a digital certificate required for network or service access allows administrators to ensure users comply to a policy for a particular network or resource in order to connect.

For example, a user is issued a Smartphone, which is provisioned to use the MDM system. An initial profile is pushed to the user's device over the air (either an open corporate access point, or through the cellular network) that sets initial configuration settings and policies such as disabling the camera, creating a link to the corporate portal or app store, or adding email account or wireless network settings. The user is now able to connect the Smartphone to the corporate network and access services according to their authorization level. If the user requires access to a secure facility and corresponding network they could connect to the MDM system and request access. An automated or administrator controlled process could then push a new profile to the device with the new security settings (disabling wireless radios, GPS, app stores, etc.) that are required for that particular building or network. The user is then allowed to access those services as long as they are in compliance with that policy. The policy could also be set by location, i.e. a Sensitive Compartmented Information Facility would require a restricted profile that was automatically enabled and disabled upon entering and exiting by the system.

The addition of mobile devices to the Army Enterprise has often been impractical due to many factors

**(Continued on page 30)**




Traditional Desktop Management

**(Continued from page 29)**

that MDM can solve. Using MDM in an enterprise solution such as the DISA DECC (much like Enterprise email) would centralize monitoring and security profile management. Access to administrative functions could be passed down to unit S6 sections, giving them powerful tools to rapidly provision, secure, track, and provide a true mobile data platform for our force. Inventory management could be simplified, as devices would be locatable through the MDM platform at all times. Lost or compromised devices could be remotely wiped by the MDM system, ensuring security of the networks and data that we use daily. As MDM continues to evolve it will most likely merge with and augment desktop management solutions, providing a holistic platform that administrators and commanders can use to ensure their network is providing necessary services in a secure and reliable manner.

**CPT Christopher J. Braunstein** *served as the lead software engineer for the Mobile Applications Branch, Accelerated Capabilities Division, Capability Development Integration Directorate, U.S. Army Signal Center of Excellence. CPT Braunstein led a team of programmers that have written nearly 100 applications for the iOS and Android platforms with over 1,500,000 downloads on iTunes and Google Play. CPT Braunstein is a graduate of the Rochester Institute of Technology with specializations in Computer Science and Information Technology. He worked for a Network-management focused consulting group as a software developer where he delivered solutions centered on the Simple Network Monitoring Protocol and network management automations. He was commissioned as an Armor officer in 2004 and served in various leadership positions to include forward support company commander, squadron adjutant, scout platoon leader, and assistant S3. CPT Braunstein deployed in support of Operation Iraqi Freedom 06-08. Upon redeployment he attended the Functional Area 53 (Information Systems Management) course, and the Signal Captains Career course.*

Join the Discussion
https://signallink.army.mil

## Acronym QuickScan

**DECC** – Defense Enterprise Computing Center
**DISA** – Defense Information Systems Agency
**GPS** – Global Positioning System
**IT** – Information Technology
**LAN** – Local Area Network
**MDM** – Mobile Device Management
**VPN** – Virtual Private Network